



Fortinet

NSE7_EFW-7.2

**Fortinet NSE 7 -
Enterprise Firewall 7.2**

Version: Demo

[Total Questions: 10]

Web: www.certsout.com

Email: support@certsout.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@certsout.com

Support

If you have any questions about our product, please provide the following items:

- ➡ exam code
- ➡ screenshot of the question
- ➡ login id/email

please contact us at support@certsout.com and our technical experts will provide support within 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

Question #:1

You want to improve reliability over a lossy IPSec tunnel.

Which combination of IPSec phase 1 parameters should you configure?

- A. fec-ingress and fec-egress
- B. Odspd and dpd-retryinterval
- C. fragmentation and fragmentation-mtu
- D. keepalive and keylive

Answer: B

Explanation

For improving reliability over a lossy IPSec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet's recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

Question #:2

Which FortiGate in a Security Fabric sends logs to FortiAnalyzer?

- A. Only the root FortiGate.
- B. Each FortiGate in the Security fabric.
- C. The FortiGate devices performing network address translation (NAT) or unified threat management (UTM), if configured.
- D. Only the last FortiGate that handled a session in the Security Fabric

Answer: B

- ➔ Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis¹². This allows you to monitor and manage the entire Security Fabric from a single console and view aggregated reports and dashboards.
- ➔ Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer. The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices³. However, it does not have to be the only log source for FortiAnalyzer.

- ➔ Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer. These devices can perform additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc⁴. However, they are not the only devices that generate logs in the Security Fabric.
- ➔ Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer. The last FortiGate is the device that terminates the session and applies the final security policy⁵. However, it does not have to be the only device that reports the session information to FortiAnalyzer. References: =
- ➔ 1: Security Fabric - Fortinet Documentation¹
- ➔ 2: FortiAnalyzer Demo⁶
- ➔ 3: Security Fabric topology
- ➔ 4: Security Fabric UTM features
- ➔ 5: Security Fabric session handling

Question #:3

After enabling IPS you receive feedback about traffic being dropped.

What could be the reason?

- A. Np-accel-mode is set to enable
- B. Traffic-submit is set to disable
- C. IPS is configured to monitor
- D. Fail-open is set to disable

Answer: D

Explanation

Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded. If fail-open is set to disable, traffic will be dropped in such scenarios¹. References: = IPS | FortiGate / FortiOS 7.2.3 - Fortinet Documentation

When IPS (Intrusion Prevention System) is configured, if **fail-open** is set to disable, it means that if the IPS engine fails, traffic will not be allowed to pass through, which can result in traffic being dropped (D). This is in contrast to a fail-open setting, which would allow traffic to bypass the IPS engine if it is not operational.

Question #:4

Refer to the exhibit.

```
config system global
  set admin-https-pki-required disable
  set av-failopen pass
  set check-protocol-header loose
  set memory-use-threshold-extreme 95
  set strict-dirty-session-check enable
  ...
end
```

which contains a partial configuration of the global system. What can you conclude from this output?

- A. NPs and CPs are enabled
- B. Only CPs are disabled
- C. Only NPs are disabled
- D. NPs and CPs are disabled

Answer: A

Explanation

The configuration output shows various global settings for a FortiGate device. The terms NP (Network Processor) and CP (Content Processor) relate to FortiGate's hardware acceleration features. However, the provided configuration output does not directly mention the status (enabled or disabled) of NPs and CPs. Typically, the command to disable or enable hardware acceleration features would specifically mention NP or CP in the command syntax. Therefore, based on the output provided, we cannot conclusively determine the status of NPs and CPs, hence option D is the closest answer since the output does not confirm that they are enabled.

Question #:5

Refer to the exhibits, which contain the network topology and BGP configuration for a hub.

Exhibit A.

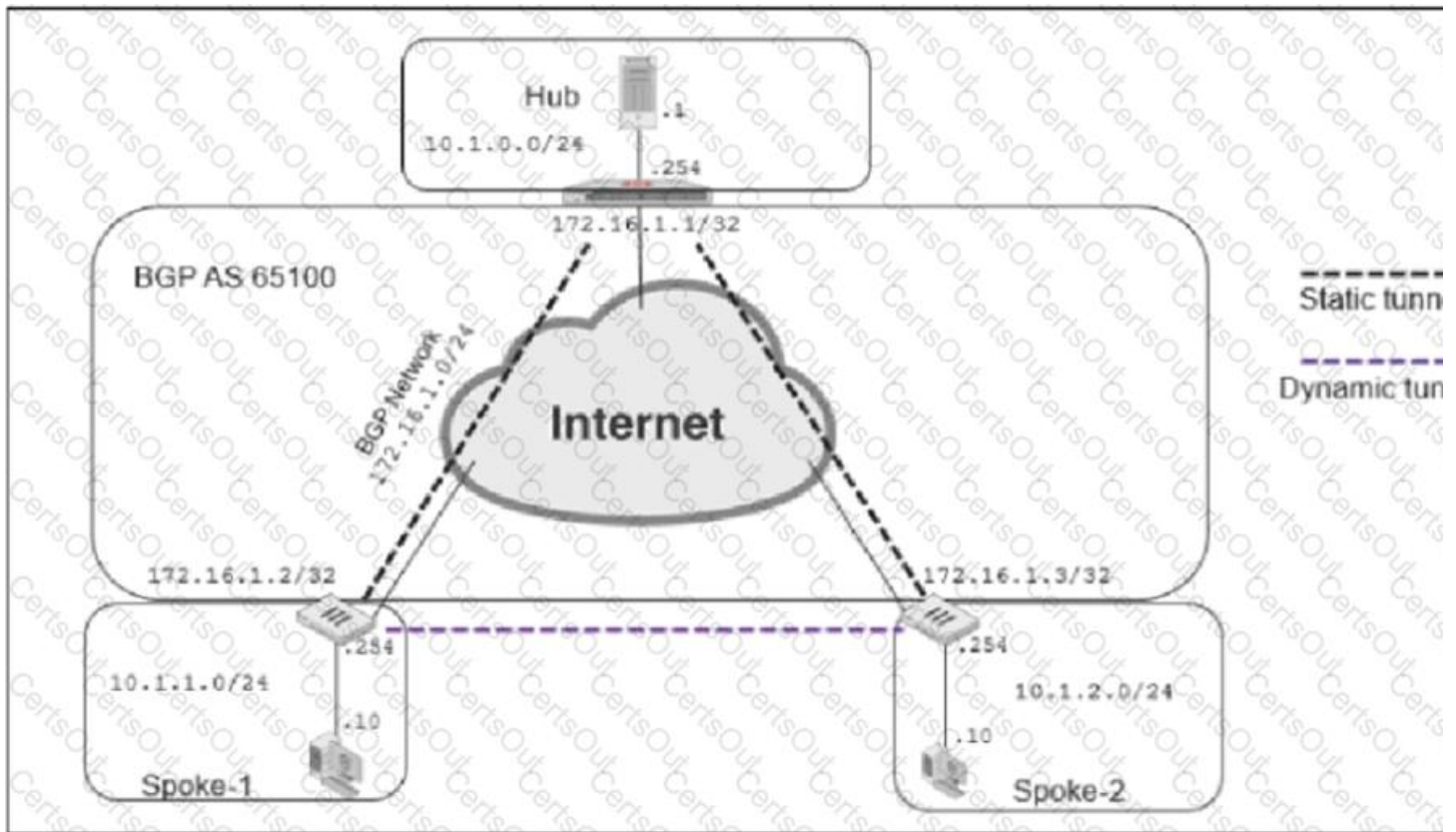


Exhibit B.

```
Hub # show router bgp
config router bgp
  set as 65100
  set router-id 172.16.1.1
  config neighbor-group
    edit "advpn"
      set remote-as 65100

      set route-reflector-client disable
    next
  end
  config neighbor-range
    edit 1
      set prefix 172.16.1.0 255.255.255.0
      set neighbor-group "advpn"
    next
  end
  config network
    edit 1
      set prefix 10.1.0.0 255.255.255.0
    next
  end
  ....
end
```

An administrator is trying to configure ADVPN with a hub and spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub is receiving route information from both spokes over iBGP; however the spokes are not receiving route information from each other.

What change must the administrator make to the hub BGP configuration so that the routes learned from one spoke are forwarded to the other spoke?

- A. Configure the hub as a route reflector
- B. Configure auto-discovery-sender on the hub
- C. Add a prefix list to the hub that permits routes to be shared between the spokes
- D. Enable route redistribution under config router bgp

Answer: B

Question #:6

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two)

- A. It can be configured as an update server a rating server or both
- B. It provides VM license validation services
- C. It supports rating requests from non-FortiGate devices.
- D. It caches available firmware updates for unmanaged devices

Answer: A B

Explanation

When deployed as a local FortiGuard Distribution Server (FDS), FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates. Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices.

Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration

Question #:7

Refer to the exhibit, which contains a partial configuration of the global system.

```
config system global
set admin-https-pki-required disable
set av-failopen pass
set check-protocol-header loose
set memory-use-threshold-extreme 95
set strict-dirty-session-check enable
..
end
```

What can you conclude from the output?

- A. set strict-dirty-session-check enable command instructs the FortiGate to offload all dirty session traffic to its SPU
- B. set check-protocol-header loose command enables hardware acceleration on this FortiGate device.
- C. set av-failopen pass command instructs the FortiGate to offload all traffic that uses the antivirus proxy to NP.
- D. set memory-use-threshold-extreme command instructs the FortiGate to disable hardware acceleration if the memory extreme threshold reaches 95%

Answer: B

Question #:8

Which ADVPN configuration must be configured using a script on FortiManager, when using VPN Manager to manage FortiGate VPN tunnels?

- A. Enable AD-VPN in IPsec phase 1
- B. Disable add-route on hub
- C. Configure IP addresses on IPsec virtual interfaces
- D. Set protected network to all

Answer: A

Explanation

To enable AD-VPN, you need to edit an SD-WAN overlay template and enable the Auto-Discovery VPN toggle. This will automatically add the required settings to the IPsec template and the BGP template. You cannot enable AD-VPN directly in the IPsec phase 1 settings using VPN Manager. References := ADVPN | FortiManager 7.2.0 - Fortinet Documentation

Question #:9

Refer to the exhibit, which shows device registration on FortiManager.

```

FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE      OID      SN      HA      IP      NAME      ADOM      IPS      FIRMWARE      Hw_GenX
unregistered 273      FGV0010000077646 - 10.1.0.1:9443 FGV0010000077646 root N/A 7.0 HR2 (1396) N/A
|- STATUS: dev-db: unknown; conf: unknown; cond: unregistered; dm: none; conn: unknown
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered 309      FGV0010000077648 - 10.1.0.100:9443 FGV0010000077648 root N/A 7.0 HR2 (1396) N/A
|- STATUS: dev-db: unknown; conf: unknown; cond: unregistered; dm: none; conn: unknown
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
unregistered 285      FGV0010000077650 - 10.1.0.253:9443 FGV0010000077650 root N/A 7.0 HR2 (1396) N/A
|- STATUS: dev-db: unknown; conf: unknown; cond: unregistered; dm: none; conn: unknown
|- vdom:[3]root flags:0 adom:root pkg:[never-installed]
fmgfaz-managed 297      FGV0010000077649 - 10.1.0.254      NGFW-1      Core 6.00741 (extended) 7.0 HR2 (1396) N/A
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
|- vdom:[3]root flags:0 adom:Core pkg:[imported]NGFW-1
fmgfaz-managed 321      FGV0010000077651 - 100.64.3.1      Spoke-1      Core 6.00741 (extended) 7.0 HR2 (1396) N/A
|- STATUS: dev-db: modified; conf: in sync; cond: Modified (recent auto-updated); dm: autoupdated; conn: up
|- vdom:[3]root flags:1 adom:Core pkg:[out-of-sync]Spokes
fmgfaz-managed 333      FGV0010000077652 - 100.64.5.1      Spoke-2      Core 6.00741 (extended) 7.0 HR2 (1396) N/A
|- STATUS: dev-db: modified; conf: in sync; cond: Modified (recent auto-updated); dm: autoupdated; conn: up
|- vdom:[3]root flags:1 adom:Core pkg:[out-of-sync]Spokes
    
```

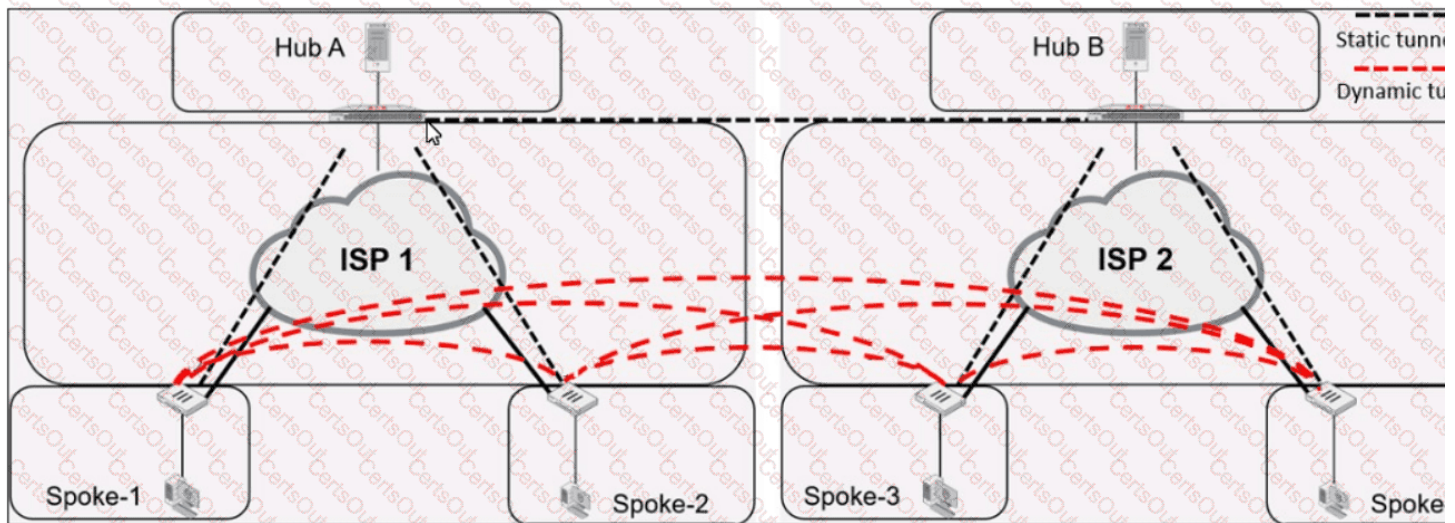
What can you conclude about the Spoke-1 and Spoke-2 configurations with respect to the information cond: Modified (recent auto-updated)?

- A. Based on the policy configuration on NGFW-1, the configuration on both spokes is modified and automatically updated.
- B. On NGFW-A, the configuration was changed and spokes are waiting for an autoupdate.
- C. On both Spoke-1 and Spoke-2, the configuration was changed directly on the FortiGate device, and the changes were automatically retrieved by the device database.
- D. Spoke-1 and Spoke-2 are sharing the same security policy configuration and the same policy package.

Answer: B

Question #:10

Refer to the exhibit, which shows an ADVPN network.



Which VPN phase 1 parameters must you configure on the hub for the ADVPN feature to function? (Choose two.)

- A. set auto-discovery-forwarder enable
- B. set add-route enable
- C. set auto-discovery-receiver enable
- D. set auto-discovery-sender enable

Answer: A C

Explanation

For the ADVPN feature to function properly on the hub, the following phase 1 parameters must be configured:

A. set auto-discovery-forwarder enable: This enables the hub to forward shortcut information to the spokes, which is essential for them to establish direct tunnels.

C. set auto-discovery-receiver enable: This allows the hub to receive shortcut offers from the spokes.

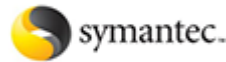
This information is corroborated by the Fortinet documentation, which explains that in an ADVPN setup, the hub must be able to both forward and receive shortcut information for dynamic tunnel creation between spokes.

About certsout.com

certsout.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: [All vendors](#)



We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- ➡ Sales: sales@certsout.com
- ➡ Feedback: feedback@certsout.com
- ➡ Support: support@certsout.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.